IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No. 17453US02

In the Application of:	
	Jeffrey D. Carr
U.S. Serial No.:	09/900,224
Filed:	July 6, 2001
For:	SYSTEM AND METHOD FOR THE CONCEALMENT OF DEVICE INPUT PARAMETERS
Examiner:	P. Parthasarathy
Group Art Unit:	2136

Confirmation No.: 4002

Cust. No.: 23446

Certificate of Transmission

I hereby certify that this correspondence is being transmitted via EFS-Web to the United States Patent and Trademark Office on November 30, 2006.

Michael T. Cruz
Reg. No. 44,636

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is a timely filed Appeal Brief. A Notice of Appeal was received by the United States Patent and Trademark Office on July 31, 2006. A Petition for a Two-Month Extension is enclosed, thereby extending the deadline by which to file an Appeal Brief to November 30, 2006.

REAL PARTY IN INTEREST

Broadcom Corporation, a corporation organized under the laws of the state of California and having a place of business at 16215 Alton Parkway, Irvine, California 92618-3616, is a real party in interest.

RELATED APPEALS AND INTERFERENCES

There are currently no appeals pending regarding related applications.

STATUS OF THE CLAIMS

Claims 1-5 and 7-18 are pending in the present application. Pending claims 1-5 and 7-18 stand rejected under 35 U.S.C. § 102(e) and are the subject of this appeal.

STATUS OF THE AMENDMENTS

An Amendment After Final Rejection was filed on July 5, 2006. In the Amendment After Final Rejection, Appellant did not amend the application. In response to the Amendment After Final Rejection, the Examiner issued the Advisory Action of July 19, 2006.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Some embodiments according to some aspects of the present invention may provide, for example, a method that conceals a parameter transferred between a first and second device as set forth in claim 1. The method may include, for example, one or more of the following: generating by the first device a control signal and a parameter signal; encrypting or hashing by the first device a portion of the control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal; transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal; receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control

signal; using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal; and generating by the second device a destination parameter signal depending upon a comparison of the control signal and the decrypted or inversely transformed control signal.

Some embodiments according to some aspects of the present invention may provide, for example, an apparatus that processes a concealed parameter received by a device as set forth in claim 7. The apparatus may include, for example, a control block and an interface operation logic block. The control logic block may receive a control signal that includes, for example, a key index and an encrypted or hashed signal that may include, for example, an encrypted or hashed form of a parameter signal and a portion of the control signal. The interface operation logic block may be operably coupled to the control logic block and may decrypt or inversely transform the encrypted or hashed signal in accordance with the key index to generate a destination parameter signal.

Some embodiments according to some aspects of the present invention may provide, for example, a method that conceals a parameter transferred between a first and second device as set forth in claim 13. The method may include, for example, one or more of the following: generating, by the first device, a control signal that may include, for example, a key index; using, by the first device, at least a portion of the control signal to obtain a first cryptographic key; encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal; transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal; receiving, by the second device from the first device, the control signal and the encrypted or hashed signal; using, by the second device, the key index from the control signal to obtain a second cryptographic key; and decrypting or inversely transforming using the second cryptographic key, by the second device, the encrypted or hashed signal to provide a decrypted or inversely transformed signal.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-5 and 7-18 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by United States Patent No. 6,118,873 to Jeffrey Bruce Lotspiech et al. ("Lotspiech").

ARGUMENT

Claims 1-5 and 7-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by United States Patent No. 6,118,873 to Jeffrey Bruce Lotspiech et al. ("Lotspiech").

I. CLAIMS 5 AND 10

The Advisory Action mailed July 19, 2006 states that claims 1-5 and 7-18 "are pending and *stay* rejected" (italics added).

It is clear from Office Action Made Final mailed May 5, 2006 that the Examiner did not intend to reject claims 5 and 10. The Office Action Made Final at page 6 states under the heading "Allowable Subject Matter" that "[c]laims 5 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims".

Thus, it is respectfully submitted to the Board that claims 5 and 10 should not have "stayed" rejected, but instead should have "stayed" objected to.

It is respectfully submitted that the Examiner or the Board clarify the status of claims 5 and 10. It is believed that claims 5 and 10 are not being rejected, but having recited patentable subject matter, are merely being objected to.

II. CLAIMS 1-4 AND 11

Claim 1 stands rejected under 35 U.S.C. § 102(e) as being anticipated by Lotspiech. To maintain the anticipation rejection, each and every element as set forth in claim 1 must be described in Lotspiech. Appellant respectfully submits that Lotspiech does not describe each and every element as set forth in claim 1.

Claim 1 recites, in part, "encrypting or hashing by the first device a portion of the

control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal; transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal; receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal".

Appellant is not entirely sure, even now, despite seeking clarifications from the Examiner, what the Examiner considers to be the control signal and what the Examiner considers to be the parameter signal as set forth in claim 1 and other claims.

Appellant respectfully requests that the Board require the Examiner to clarify what the Examiner considers the control signal in Lotspiech and what the Examiner considers the parameter signal as well as other elements as set forth in claim 1 and other claims.

In the Office Action Made Final mailed May 5, 2006, the Examiner states "[a] session number is encrypted with the device key and then transmitted for used in decrypting program".

Since claim 1 recites "encrypting ... by the first device a portion of the control signal with the parameter signal to generate an encrypted ... parameter signal and control signal", Appellant will assume that the Examiner is alleging that the SESSION NUMBER x_i of Lotspiech corresponds to A PORTION OF THE CONTROL SIGNAL as set forth in claim 1. Appellant neither agrees nor disagrees with such an assumption. Appellant is merely discussing what appears to be the Examiner's allegation who has the initial burden of going forward.

As discussed in the Response to the Office Action Made Final dated July 5, 2006, the problem with the session number x_i of Lotspiech corresponding, as alleged by the Examiner, to a portion of the control signal as set forth in claim 1 is that claim 1 recites "transmitting by the first device to the second device the control signal and the encrypted ... parameter signal and control signal".

If the session number x_i is a portion of the control signal as alleged by the Examiner, then the Examiner is alleging that the source 16 in Lotspiech is transmitting (1) the alleged

control signal including the session number x_i and (2) the encrypted parameter signal and control signal.

Appellant then respectfully drew the attention of the Examiner to the fact that Lotspiech does not describe the source 16 transmitting (1) the session number and (2) the encrypted parameter signal and session number. (*Respectfully, it would be useful for the Board and Appellant to know with clarify what the Examiner considers the parameter signal.*)

The Advisory Action mailed July 19, 2006 states that the "Examiner respectfully directs to Lotspiech Column 5 line 55 – Column 6 line 41, in particular, to the detail discussion of items 44 and 46". Advisory Action mailed July 19, 2006 at page 2.

As per the direction of the Examiner, Appellant respectfully draws the attention of the Board to items 44 and 46.

Item 44 is a block in the process illustrated in FIG. 4 of Lotspiech.

Item 46 is a Calculate Session Key Message 46 as illustrated in FIG. 6 of Lotspiech.

The block 44 in FIG. 4 of Lotspiech states "Insert session key block at start of broadcast program; Xmit Message". The session key block 42 is illustrated in FIG. 5 of Lotspiech.

The session key block 42 is a matrix containing *encrypted* versions of each session number x_i. See Lotspiech at col. 5, line 66 to col. 6, line 2.

Indeed, in FIG. 6 of Lotspiech, the Calculate Session Key Message 46 does illustrated session key block 52.

Thus, in view of the Examiner's allegation, the Examiner appears to be alleging that encrypted versions of session number x_i are in the session key block 52 of Calculate Session Key Message 46.

However, neither item 44 nor item 46 contemplates sending (1) a session number and (2) an encrypted parameter signal and session number as alleged by the Examiner.

In view of the Examiner's allegation, Lotspiech at col. 5, line 55 to col. 6, line 41 only allegedly supports sending an encrypted session number in the Calculate Session Key Message 46. Lotspiech at col. 5, line 55 to col. 6, line 41 does not support sending (1) a session number and (2) an encrypted parameter signal and session number.

Thus, even the Examiner's allegation falls short of describing each and every element as set forth in claim 1 in support of an anticipation rejection of claim 1.

For at least the above reasons, it is therefore respectfully requested that the Board reverse the rejection of claim 1 and its rejected dependent claims (i.e., claims 2-4 and 11).

III. CLAIMS 7-9 and 12

Claim 7 stands rejected under 35 U.S.C. § 102(e) as being anticipated by Lotspiech. To maintain the anticipation rejection, each and every element as set forth in claim 7 must be described in Lotspiech. Appellant respectfully submits that Lotspiech does not describe each and every element as set forth in claim 7.

Claim 7 recites, in part, "a control logic block to receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal".

In support of the rejection, the Examiner relied on Lotspiech at col. 6, lines 3-32. See Office Action Made Final mailed May 5, 2006 at pages 5 and 6.

In the Office Action Made Final mailed May 5, 2006 at page 6, the Examiner alleges that Lotspiech at col. 6, lines 3-32 describes a device that "receives the session key and encrypted data". See Office Action Made Final mailed May 5, 2006 at page 6.

In view of the Examiner's other allegations, Appellant can only guess that the Examiner believed the key index as set forth in claim 7 to be the session number x_i of Lotspiech. Appellant can neither confirm nor deny that the key index as set forth in claim 7 corresponds to the session number x_i of Lotspiech and is only attempting to interpret the Examiner's sparse allegations.

As discussed above with respect to claim 1, the device 18 or 20 does not receive the session number x_i in Calculate Session Key Message 46. Instead, Calculate Session Key Message 46 contains a session key block 52 which is a matrix containing *encrypted* versions of each session number x_i. See Lotspiech at col. 5, line 66 to col. 6, line 2.

Thus, even the Examiner's allegation falls short of describing each and every element as set forth in claim 7 in support of an anticipation rejection of claim 7.

For at least the above reasons, it is therefore respectfully requested that the Board reverse the rejection of claim 7 and its rejected dependent claims (i.e., claims 8, 9 and 12).

IV. CLAIMS 13-18

Claim 13 stands rejected under 35 U.S.C. § 102(e) as being anticipated by Lotspiech. To maintain the anticipation rejection, each and every element as set forth in claim 13 must be described in Lotspiech. Appellant respectfully submits that Lotspiech does not describe each and every element as set forth in claim 13.

Claim 13 recites, in part, "generating, by the first device, a control signal comprising a key index; using, by the first device, at least a portion of the control signal to obtain a first cryptographic key; encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal; transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal".

Again, there is nothing definitive from the Examiner as to which elements in claim 13 correspond to components in Lotspiech. In view of the Examiner's other allegations, Appellant can only guess that the Examiner believed the key index as set forth in claim 13 to be the session number x_i of Lotspiech as may have been previously alleged. Appellant can neither confirm nor deny that the key index as set forth in claim 13 corresponds to the session number x_i of Lotspiech and is only attempting to interpret the Examiner's sparse allegations.

However, as pointed out above with respect to claims 1 and 7, the session number x_i is not in Calculate Session Key Message 46. Instead, Calculate Session Key Message 46 contains a session key block 52 which is a matrix containing *encrypted* versions of each session number x_i. See Lotspiech at col. 5, line 66 to col. 6, line 2.

Thus, even the Examiner's allegation falls short of describing each and every element as set forth in claim 13 in support of an anticipation rejection of claim 13.

For at least the above reasons, it is therefore respectfully requested that the Board reverse the rejection of claim 13 and its rejected dependent claims (i.e., claims 14-18).

CONCLUSION

For the foregoing reasons, claims 1-5 and 7-18 are distinguishable over the prior art of record. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge additional fees or credit overpayments to the deposit account of McAndrews, Held & Malloy, Account No. 13-0017.

Dated: November 30, 2006

Respectfully submitted,

Michael T. Cruz
Registration No. 44,636

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775-8100

CLAIMS APPENDIX

The following claims are involved in this appeal:

1. A method for concealing a parameter transferred between a first and second device, comprising:

generating by the first device a control signal and a parameter signal;

encrypting or hashing by the first device a portion of the control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal;

transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal;

receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal;

using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal; and

generating by the second device a destination parameter signal depending upon a comparison of the control signal and the decrypted or inversely transformed control signal.

2. The method of claim 1, further characterized by:

generating by the first device a first key signal using the control signal; and

wherein encrypting or hashing comprises using the first key signal.

3. The method of claim 2, further characterized by:

generating by the second device a second key signal using the control signal; and

generating by the second device the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the second key signal.

4. The method of claim 3, further characterized by:

generating by the first device a key index signal;

generating by the first device a key variable signal;

transmitting by the first device to the second device the key index signal and the key variable signal;

receiving by the second device from the first device the key index signal and the key variable signal;

generating by the second device an intermediate key signal using the key index signal and a key table; and

generating by the second device the second key signal using the intermediate key signal and the key variable signal.

5. The method of claim 4, further characterized by generating by the second device the second key signal from the intermediate key signal and the key variable signal using a hash function.

7. An apparatus for processing a concealed parameter received by a device, comprising:

a control logic block to receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal; and

an interface operation logic block operably coupled to the control logic block to decrypt or inversely transform the encrypted or hashed signal in accordance with the key index to generate a destination parameter signal.

8. The apparatus of claim 7, further characterized by:

a key table module including indexed cryptographic keys, the key table module operably coupled to the control logic block, the key table module to generate a key signal using the control signal; and

an inverse transformation module operably coupled to the key table module and the control logic block, the inverse transformation module to generate the destination

parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the key signal.

9. The apparatus of claim 7, further characterized by:

a key table module including indexed cryptographic keys, the key table module operably coupled to the control logic block, the key table module to generate an intermediate key signal using a key index signal received from the control logic block;

a key interface stage operably coupled to the key table module and the control logic block for generating a key signal using the intermediate key signal received from the key table module and a key variable signal received from the control logic block; and

an inverse transformation module operably coupled to the key interface stage and the control logic block, the inverse transformation module to generate the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the key signal received from the key interface stage.

10. The apparatus of claim 9 further characterized by a hash function stage operably coupled to the key interface stage, the hash function stage to generate the key signal from the intermediate key signal and the key variable signal.

11. The method of claim 1, wherein the control signal comprises a key index and the portion of the control signal comprises the key index.

12. The apparatus of claim 7, wherein the portion of the control signal comprises the key index.

13. A method for concealing a parameter transferred between a first and second device, characterized by:

generating, by the first device, a control signal comprising a key index;

using, by the first device, at least a portion of the control signal to obtain a first cryptographic key;

encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal;

transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal;

receiving, by the second device from the first device, the control signal and the encrypted or hashed signal;

using, by the second device, the key index from the control signal to obtain a second cryptographic key; and

decrypting or inversely transforming using the second cryptographic key, by the second device, the encrypted or hashed signal to provide a decrypted or inversely transformed signal.

14. The method of claim 13, wherein:

the first signal comprises a parameter signal and a portion of the control signal;

the decrypted or inversely hashed signal comprises a decrypted or inversely transformed portion of the control signal and a decrypted or inversely transformed parameter signal; and

the second device stores the decrypted or inversely transformed parameter signal depending on a comparison of a portion of the control signal received from the first device and the decrypted or inversely transformed portion of the control signal.

15. The method of claim 14, wherein the decrypted or inversely transformed portion of the control signal comprises the key index.

16. The method of claim 13, comprising:

transmitting, by the first device to the second device, a destination register signal;

receiving, by the second device from the first device, the destination register signal;

storing, by the second device, at least a portion of the decrypted or inversely transformed signal at a location determined in accordance with the destination register

signal.

17. The method of claim 13 wherein using at least a portion of the control signal to obtain a first cryptographic key comprises using the key index as an index into a data memory to retrieve the first cryptographic key from the data memory.

18. The method of claim 13 wherein the key index comprises an index into a data memory that is used to retrieve the second cryptographic key from the data memory.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.